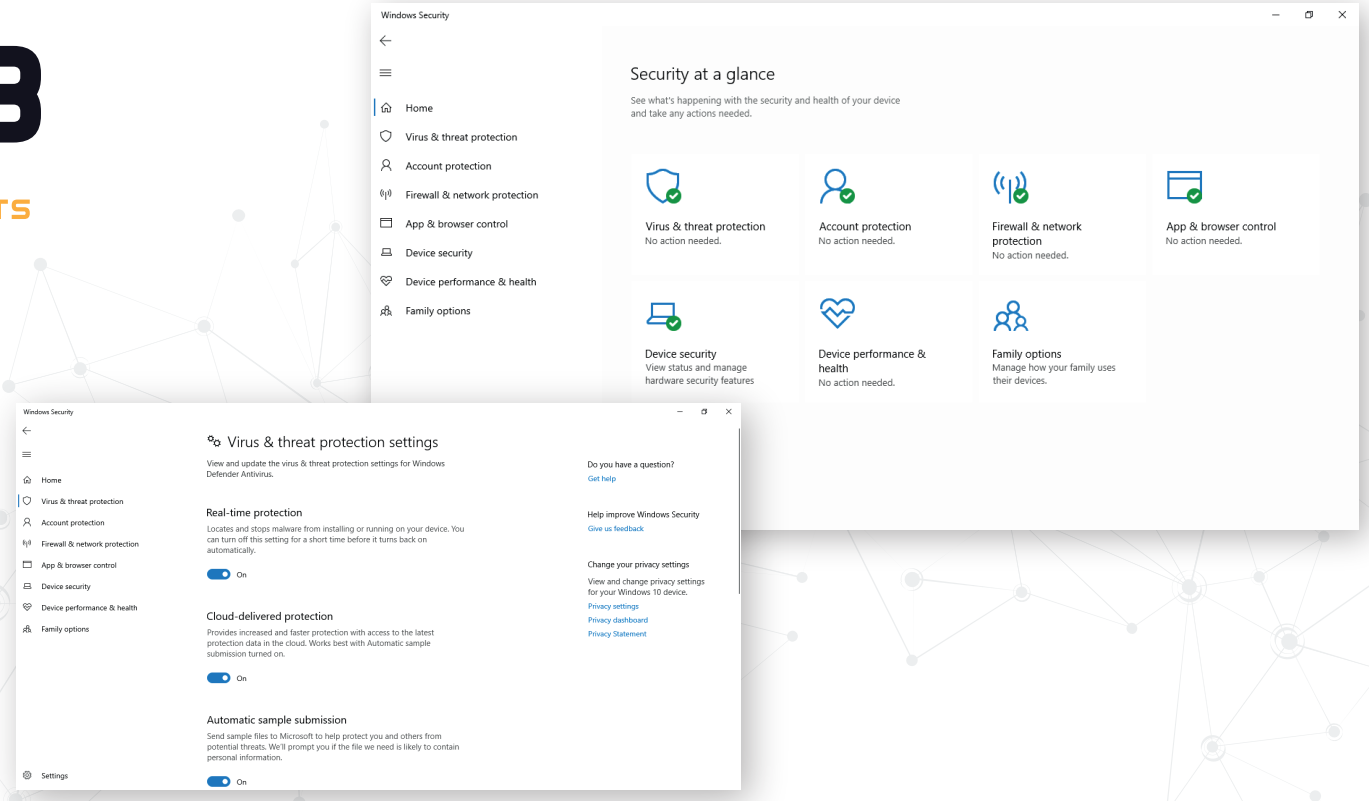
AV-TEST LAB

THE INDEPENDENT ANTIVIRUS TESTS



Product name: WINDOWS Defender Antivirus

Date of the test: April 2020

The best antiviruses based on test of protection against fileless attacks, ransomware, and macro viruses

Main objectives of the test

The verification of security effectiveness of popular applications to protect personal computers and workstations against most common threats and cyberattacks since the beginning of 2020.

In the last quarter, cybercriminals understood that in order to avoid detection by traditional security tools, they need to combine popular types of malicious software with modern techniques of attacking. According to the reports of global IT companies, fileless attacks will be very a common phenomenon in the coming quarters. Using this type of security deception has increased by several hundred percent as Trend Micro observed in late December 2019. Tools to automatic search vulnerabilities in applications programmed by hackers are now more technically capable than before. They are also harder to observe because require no user interaction in order to execute malicious code.

Destroying the work of universities, public hospitals, and private clinics that try together to isolate diseases, is an acute problem. It is difficult to understand what primitive motives are driven by criminals, and why they turn against science and healthcare. The actions of online criminals have negative consequences in the economy as we could observe in recent weeks. Major news services wrote about incidents of forcing ransom healthcare and education institutions in exchange for encrypting data lost as a result of a cyberattack.

Trends in cyberthreats in 2020 underline the need for invest in solutions that will allow users to provide detailed reporting of significant changes to systems and networks. Developers and providers of IT solutions should take responsibility for solutions that are provided to companies and end users. On the other hand, enterprises must understand the risk, and start to protect themselves proactively against attack, and also mitigate the effects of potential attacks. Most organizations cannot afford to keep basic security to protect network, not to mention maintaining 24-hour units of monitoring infrastructure security. Companies should consider collaborating with an experience provider of security services who will help them protect IT systems against modern cyberattacks.

Malicious Office documents

Macros can be easily connected to sociotechnical techniques in phishing campaigns. Document circulation in enterprises is a normal thing, and the Office suit installed by default forces us to protect IT systems against the attempt of infecting systems.

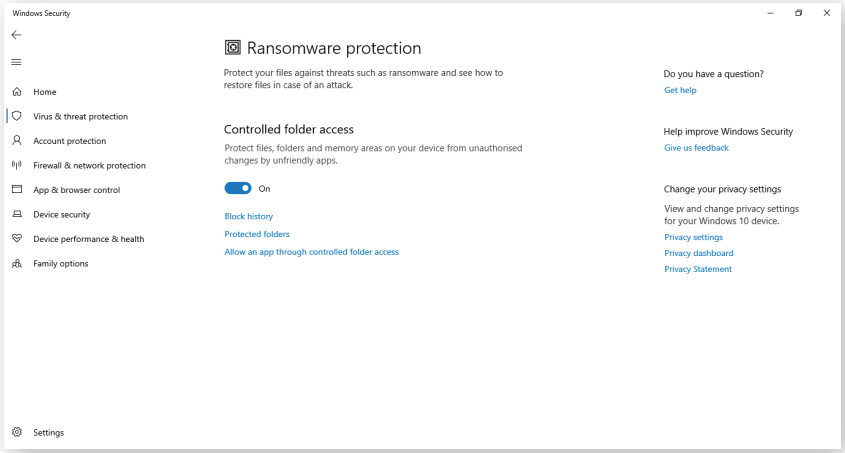
Ransomware attacks

An organization that will lose an access to the data can have not only a serious P.R. problem, but also financial due to penalties imposed by the so called RODO. Attacks involving ransomware samples are still popular. Hackers focus mainly on medium and large organizations without excluding public institutions. And now they are not trying to extort ransom in exchange for data decryption. Criminal activities become more menacing because of increasing trade of stolen files content on forums in Tor network.

Techniques of fileless infecting of IT systems

Modern operating systems already have built-in tools used by criminals, and so they do not need to install malicious software. A script in PowerShell is easy to obfuscate, and therefore cannot be detected using older security tools. Administrators commonly use PowerShell to automate certain activities, and functioning of system processes, such as PowerShell or Windows Management Instrumentation is not unusual a corporate environment.

Hackers have a great scope of activity in targeted campaigns because they prepare to attack carefully. Typically, “a cyberattack lifecycle” is as follows: first, a target is recognized, then tools are adapted to victim’s IT system. The last step is to attack and break the chain. Targeted attacks of ATP (Advanced Threat Persistence) are more difficult to detect and stop. Unconventional techniques of bypassing security, if used in a controlled environment, they can tell a lot about protection effectiveness of a given product. Criminals care most about the money, this is why the majority of campaigns are directed to the masses. IT systems which are protected with recommended solutions, are in the advantageous position to an attacker.



Product name: WINDOWS Defender Antivirus
Date of the test: April 2020

Windows Defender as an integral part of Windows systems does not provide a good protection against macro viruses and ransomware. The antivirus works with the SmartScreen system function that analyses files downloaded from the Internet and applications from the Microsoft Store for the source, checksums, and blacklist patterns which are provided by Microsoft to Windows Defender as signatures. The antivirus lacks more advanced techniques to analyze new malicious code. Harmful commands executed in PowerShell could be subjected to higher restrictions.

Technical details

LEVEL 1	L1	The browser level, i.e. a virus has been stopped before or after it has been downloaded onto a hard drive.
LEVEL 2	L2	The system level, i.e. a virus has been downloaded, but it has not been allowed to run.
LEVEL 3	L3	The analysis level, i.e. a virus has been run and blocked by a tested product.
FAIL	F	The failure, i.e. a virus has not been blocked and it has infected a system.

NO.	MACRO VIRUSES	FILE NAME	WINDOWS Defender Antivirus
1	c141a187c5b2c7a8d91a923a0f79a8ba4c1484e7295f922c5fac3d7c0d6792b9	1.doc	L3
2	276e5e230766222ed208b1d4d1bd994acc2e763ca71c6d28f41a17988375d099	2.doc	L3
3	23a4d7782a91e2a297f8b082500a6036048940afbee12a951dc02da2a0004ec2	3.doc	L3
4	6bed7ef049d8d9728a09a94488ac8670c9c20c0e6c294f80fd2153c37a2bead7	4.doc	L3
5	dc0699e81874193e461b6a2ca9bf7164c2fe4d214381d1b5b875203541efcab7	5.doc	L3

To learn more about technical details, please contact us.

Technical details

LEVEL 1	L1	The browser level, i.e. a virus has been stopped before or after it has been downloaded onto a hard drive.
LEVEL 2	L2	The system level, i.e. a virus has been downloaded, but it has not been allowed to run.
LEVEL 3	L3	The analysis level, i.e. a virus has been run and blocked by a tested product.
FAIL	F	The failure, i.e. a virus has not been blocked and it has infected a system.

NO.	MACRO VIRUSES	FILE NAME	WINDOWS Defender Antivirus
1	3320f11728458d01eef62e10e48897ec1c2277c1fe1aa2d471a16b4dccfc1207	1.exe	L3
2	3299f07bc0711b3587fe8a1c6bf3ee6bcbc14cb775f64b28a61d72ebcb8968d3	2.exe	L2
3	86456ebf6b807e8253faf1262e7a2b673131c80174f6133b253b2e5f0da442a9	3.exe	F
4	9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1	4.exe	F
5	4e6c191325b37da546e72f4a7334d820995d744bf7bb1a03605adb3ad30ce9ca	5.exe	L1

To learn more about technical details, please contact us.

Technical details

	FILELESS ATTACKS	FILE NAME	WINDOWS Defender Antivirus
POWERSHELL	c1525592fdf22f2ea068b5e2428d5e36fd9629ef8f5dd648ee792b4cb936fe53	1.bat	Threat has been run, but the firewall has blocked a connection with hacker's server
MSHTA	e43ac1a50122d5f8584d21d768ea171d1f5f78075bbb73ae178506b6f8d071cb	2.hta	Threat has been launched, but raised the alarm of antivirus

To learn more about technical details,
please contact us: kontakt@avlab.pl

Product name: WINDOWS Defender Antivirus
Date of the test: April 2020

Granted recommendations in categories

Protection
against malicious
Office documents

Blocked threats
in the wild **65/65**

Protection
against
encrypting data

Blocked threats
in the wild **24/24**

Protection
against
fileless attacks

Blocked scenarios
of attacks **2/2**

AVLab is an independent organization as guardian of Internet security that provides information from the industry through articles, reportage from training and conferences. Our distinctive feature are reviews and security tests. In our tests we use malicious software, tools, and techniques of bypassing security that are used in real attacks.

Developers may send their enquiries for more technical details at: kontakt@avlab.pl